

Mobile Payment System Project

PayMobile 2.0
February-March 2010

История изменений

| Дата | Автор | Описание |
|------------|--------------|-------------------|
| 01.02.2010 | Тулупов Е.А. | Начало разработки |
| | | |
| | | |
| | | |

Оглавление

| | | |
|-----|--|----|
| 1 | Сокращения..... | 4 |
| 2 | Общие положения..... | 4 |
| 2.1 | Мидлет..... | 5 |
| 3 | Общая схема..... | 5 |
| 4 | Концепция..... | 6 |
| 4.1 | Регистрация и инициализация..... | 6 |
| 4.2 | Совершение операции..... | 7 |
| 4.3 | Серверная архитектура..... | 7 |
| 5 | Подключение к услуге..... | 8 |
| 6 | Подача запроса на обслуживание..... | 10 |
| 7 | Контроллер запросов на обслуживание..... | 11 |
| 7.1 | Обработка уведомлений..... | 12 |
| 7.2 | Исполнение запроса..... | 12 |
| 7.3 | Проверка подписи и контракта..... | 13 |
| 7.4 | Отмена запроса..... | 14 |
| 8 | Интерфейсы..... | 15 |
| 8.1 | Запрос..... | 15 |
| 8.2 | Ответ..... | 16 |
| 9 | Настройки мидлета..... | 16 |
| 10 | Отчетность..... | 17 |
| 11 | Безопасность..... | 17 |
| 12 | Обязательства покупателя..... | 19 |
| 13 | Требования системы..... | 20 |
| 14 | Чек лист..... | 20 |

1 Сокращения

| | |
|-------|--------------------------------------|
| ВДО | Select For Update DML. |
| ЗИД | Защитный Идентификатор Договора. |
| ЗО | Запрос на Обслуживание. |
| ИАП | Идентификатор Алгоритма Подписи. |
| ИКМК | Индекс КМК. |
| ИП | Идентификатор Процессора. |
| КЗО | Контроллер Запросов на Обслуживание. |
| КМК | Корневой МК. |
| МК | Мастер Ключ. |
| СЖ | Системный Журнал. |
| СМПП | SMPP. |
| СМС | SMS. |
| СП | Счетчик Подписей. |
| СЧ | Случайное Число. |
| ХТТПС | HTTPS соединение. |
| ШС | Шифрованное TLS/SSL Соединение. |

2 Общие положения

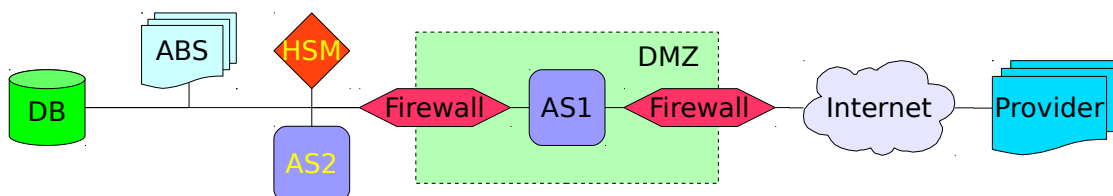
1. От системы должна быть польза людям.
2. Предлагая систему нужно, чтобы покупатель сам определил ее стоимость — лицензии и годового сопровождения. Например, в разрезе периодов (кварталов/годов):
 1. определить тарифы по каждому виду операции;
 2. определить вероятное количество операций;
 3. рассчитать предполагаемый доход;
 4. определить амортизацию по каждому виду инвестиций;
 5. определить операционные расходы;
 6. рассчитать точку окупаемости.

Либо самому произвести расчет, с учетом конъюнктуры, и предоставить его покупателю, предварительно получив от последнего желаемые тарифы и предполагаемое количество операций.

2.1 Мидлет

1. До передачи покупателю мидлета, последний должен быть персонализирован адресом и иконкой покупателя.
2. ШС устанавливается с использованием (предварительно) интерфейса `javax.microedition.io.SecureConnection` и класса `javax.net.ssl.SSLServerSocket`.

3 Общая схема

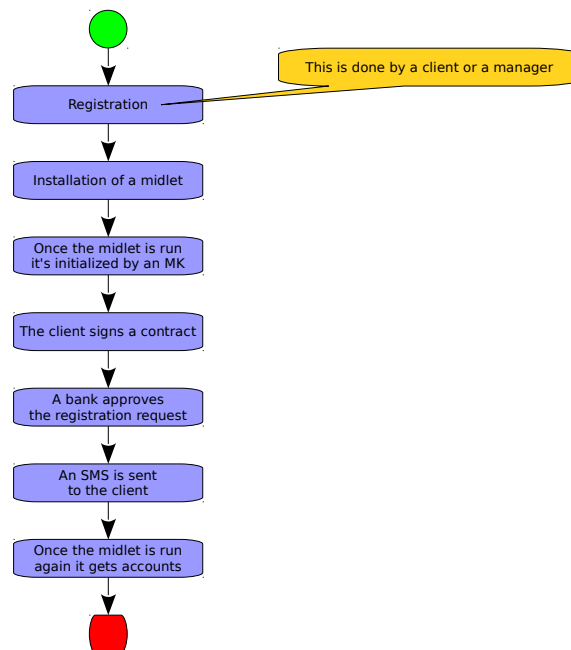


Примечания:

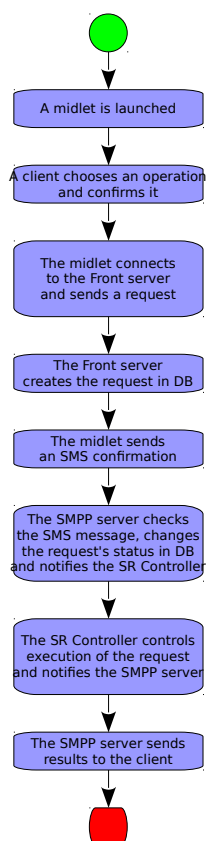
1. AS1 — регистрация клиентов, фронтальный сервер, СМПП сервер;
2. AS2 — веб интерфейс для персонала (с большим доступом к БД), КЗО, интерфейсы;
3. HSM — карточный крипто-модуль;
4. если крипто-модули серверов AS1 и AS2 приемлемы (внутренняя генерация, двойной контроль и т. д.) в части симметричных алгоритмов, то HSM не нужен;
5. ABS – банковская, карточная и т. д. системы;
6. Provider – телекоммуникационные, телевизионные и прочие операторы.

4 Концепция

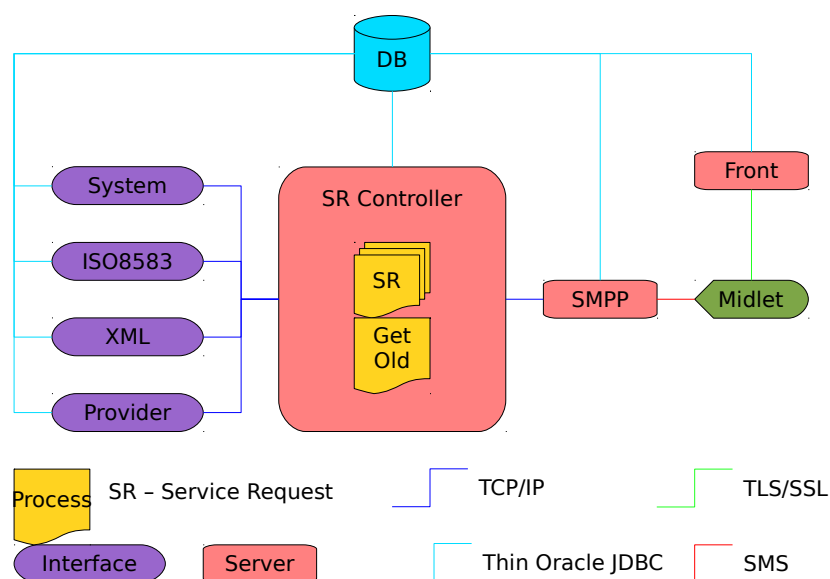
4.1 Регистрация и инициализация



4.2 Совершение операции



4.3 Серверная архитектура



Примечания:

Никакая часть настоящего документа не может быть воспроизведена или передана в какой бы то ни было форме или какими то ни было средствами, электронными или механическими, для какой бы то ни было цели, без письменного разрешения компании PaySoft.

1. ЗО после обработки конкретного шага/этапа завершается;
2. интерфейсы фиксируют все сообщения;
3. интерфейс System обслуживает тип запроса «Обновление № счетов»;
4. СМПП сервер при успешной отправке уведомления устанавливает в запросе статус отправки «Отправлено», при ошибке — «Ошибка»;
5. Get Old периодически выбирает незавершенные запросы со сроком больше тайм аута + величина, увеличиваемая в геометрической прогрессии, и уведомляет КЗО о необходимости их очистки.

5 Подключение к услуге

Ниже приводится последовательность, при которой клиент самостоятельно регистрируется. По причине безопасности, сокращения расходов (уменьшения количества оборудования и ПО) или по иным причинам регистрацию может производить банковский сотрудник, сообщая клиенту, что и когда делать на телефоне.

1. Клиент входит на сайт регистрации.
2. Клиент уведомляется о том, что он должен:
 1. выписать полный адрес текущей страницы и убедиться в наличии безопасного соединения, т. е. наличия замочка (озеленения цвета поля для ввода адреса), отсутствии предупреждений браузера;
 2. удалить старый неиспользуемый мидлет этой системы и этого банка, если таковой имеется;
 3. зайти с телефона на определенный сайт, убедиться в защищенности связи, скачать и установить мидлет. Возможно, нужно будет еще запустить мидлет с тем, чтобы отобразить № телефона, если формат №, получаемый мидлетом, иной от человеко-читаемого.
3. Клиент вносит (звездочкой помечены обязательные поля):
 1. персональные данные:
 1. фамилия, имя и отчество;
 2. дата рождения;
 3. страна*;
 4. тип документа*;
 5. № документа*;
 6. дата выдачи документа;
 7. кем выдан документ;
 8. адрес;
 9. РНН.

2. № телефона*;
3. филиал*;
4. типы, виды (отправитель/получатель), № счетов, транзакционные (разовый, суточный, месячный – по сумме и количеству) и временные (со столько-то до столько) ограничения (включительно) по каждому из них.

Эти данные записываются в таблицы заявок (дата подачи и статус «Ожидание инициализации» устанавливаются по умолчанию) и транзакционных/временных ограничений на (пере)подключение к услуге.

4. Клиенту выводиться № заявки и сообщение о необходимости запустить мидлет.
5. Т. к. нет МК, то происходит процедура его автоматической загрузки:
 1. мидлет подключается по ШС;
 2. мидлет запрашивает у клиента № заявки и сохраняет его, как ЗИД;
 3. мидлет делает запрос на инициализацию (№ заявки и телефона);
 4. сервер ВДО заявку со статусом «Ожидание инициализации» по № заявки и телефона, если количество записей не равно 1:
 1. то СЖ, отвечает кодом «Системная ошибка» и разрывает ШС;
 2. иначе изменяет статус заявки на «Инициализация» и отвечает кодом «Успешно».
 5. клиент вводит 2 раза маскированный или 1 раз открытый¹ пароль в мидлете, который отправляет его на сервер;
 6. сервер проверяет пароль на сложность, если он не удовлетворяет критериям:
 1. то отвечает кодом «Ошибка проверки пароля» (ограничить количество попыток);
 2. иначе заявку в «Подано», отправляет МК, ИКМК, ИАП, Соль, код «Успешно» и разрывает ШС.
6. Клиент приходит в отделение банка.
7. Менеджер находит заявку клиента, проверяет/сверяет данные заявки.
8. Клиент подписывает договор, где есть пункт о том, что клиент произвел регистрацию и загрузку мидлета с определенного(ых) банком сайта(ов) (в адресе выделить либо ХТТПС или ХТТПС) (см. п. 2).
9. При подтверждении заявки система (в рамках Oracle FMW Task Flow):
 1. начинает транзакцию;
 2. ВДО заявку со статусом «Подано»;

1 Это может понадобиться, т. к. на обычных телефонных клавиатурах на одну клавишу привязаны несколько символов. Если активирована глобальным параметром, включаемый по требованию заказчика, то для клиента должна быть возможность выбрать между этими двумя вариантами.

3. ВДО клиента по стране, типу и № документа, если возвращаемый набор записей пустой, то переходит к следующему шагу, иначе выводит информацию о существующем клиенте, где менеджер проверяет соответствие данных существующего клиента с клиентом, подающим заявку и при:
 1. совпадении подтверждает создание договора под существующим клиентом;
 2. не совпадении корректирует заявку или отклоняет ее с указанием причины.

Рассмотреть возможность установки тайм аута на этом шаге;
4. ВДО договор по № телефона и проверяет заведен ли уже такой:
 1. договор со статусом не «Закрыт». Если да, то выводится уведомление «Существует не закрытый договор» с отказом в дальнейшей обработке;
 2. клиент. Если:
 1. заведен, то создается новый договор со статусом «Блокирован» под существующим клиентом;
 2. не заведен, то создается новый клиент с новым договором со статусом «Блокирован».
5. закрывает заявку с указанием даты закрытия и статуса «Принято»;
6. совершает транзакцию.
10. Менеджер нажимает кнопку «Проверить», если все верно, то статус в «Проверен».
11. Контролер одобряет договор — статус изменяется на «Одобен» только, если нет других договоров с таким же № телефона и статусом не «Закрыт».
12. Клиенту отправляется СМС уведомление о подключении к услуге.
13. Клиент запускает мидлет. Т. к. нет № счетов, то происходит процедура их автоматического получения.


6 Подача запроса на обслуживание

1. Клиент запускает мидлет.
2. Клиент выбирает/вводит (звездочкой помечены обязательные поля):
 1. «Переводы»:
 1. № счета отправителя* (выводимых по фильтру “S”);
 2. № счета получателя* (выводимых по фильтру “R”);
 3. сумму*
 4. валюту*;
 5. КНП;
 6. описание.

2. «Предопределенные переводы»:
 1. наименование предопределенного перевода (см. раздел 9):
 1. те же поля, что и в пункте «Переводы» выше.
3. «Выписка»:
 1. № счета* (выводимых по фильтру “S”);
 2. тип выписки*.
4. «Остаток счета»:
 1. № счета* (выводимых по фильтру “S”).
5. в настройках «Обновить счета».
3. Клиент нажимает кнопку «Выполнить» (за исключением обновления счетов).
4. Мидлет соединяется по ШС.
5. Мидлет запрашивает СЧ.
6. Сервер отвечает СЧ и кодом «Успешно».
7. Мидлет подписывает данные операции и отправляет запрос на обслуживание.
8. Сервер проверяет СЧ, создает запрос на обслуживание, отвечает идентификатором запроса, кодом «Успешно». В соответствии со справочником типов ЗО разрывает ШС.
9. Если мидлет получает код «Успешно», то отправляет идентификатор запроса по СМС.
10. СМПП сервер по идентификатору ВДО запрос. Если количество записей равно «1»:
 1. то, проверив соответствие № телефона, уведомляет КЗО;
 2. иначе СЖ.
11. СМПП сервер, в зависимости от настроек системы, отправляет результаты мидлету и удаляет активный запрос.
12. Если тип запроса не «Перевод», то мидлет отправляет запрос на ожидание обработки.
13. Сервер, как продолжение сессии с типом запроса не «Перевод», периодически проверяет запрос и если он успешен:
 1. то отвечает информацией из него, кодом «Успешно» и разрывает ШС;
 2. иначе отвечает кодом «Системная ошибка» и разрывает ШС.
14. Если тип запроса не «Перевод», то мидлет выводит информацию.

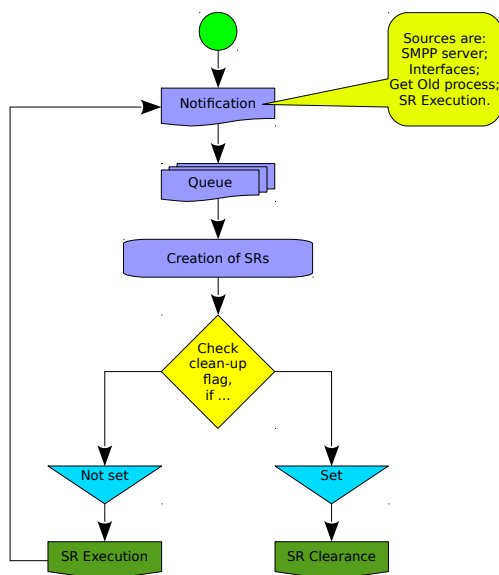
7 Контроллер запросов на обслуживание

В нижеприведенных схемах подразумевается, что:

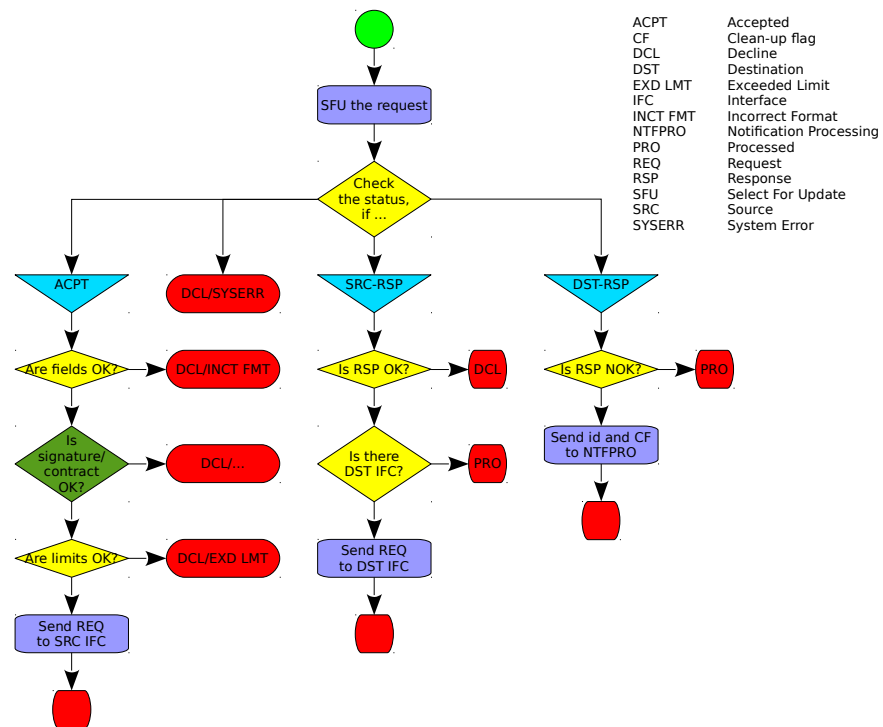
1. при завершении без действий (т. е. — ) производится только откат;
2. при завершении с установлением статуса:

1. «Отклонен» (т. е. — **DCL/INCT FMT**, и т. п., кроме — **PRO**) СЖ (при необходимости);
2. совершается транзакция.
3. поле «Причина отказа» обновляется только, если оно пустое.

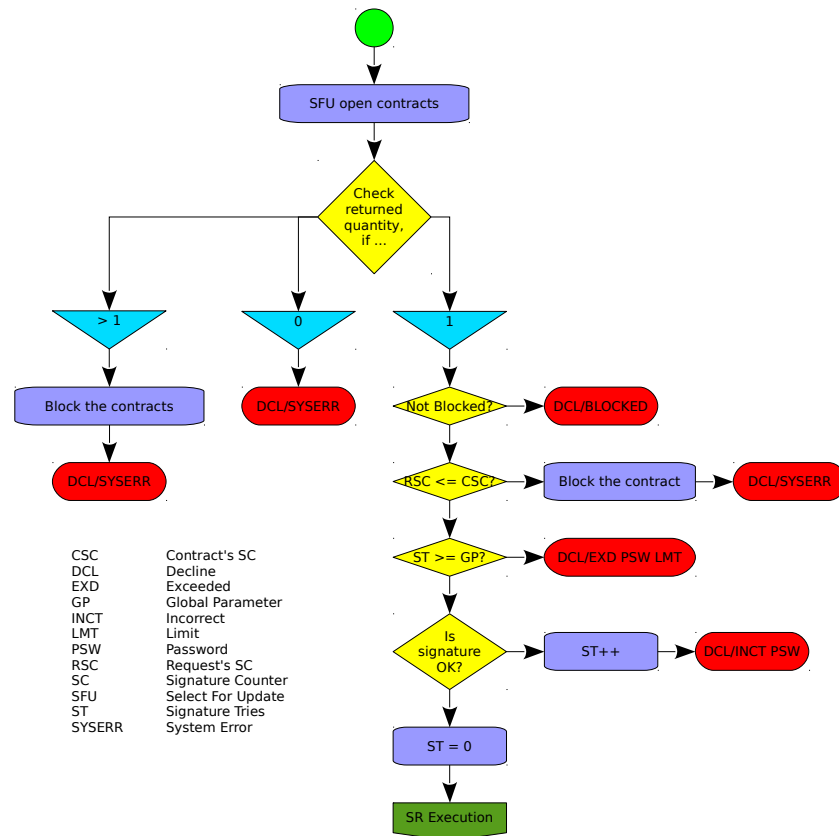
7.1 Обработка уведомлений



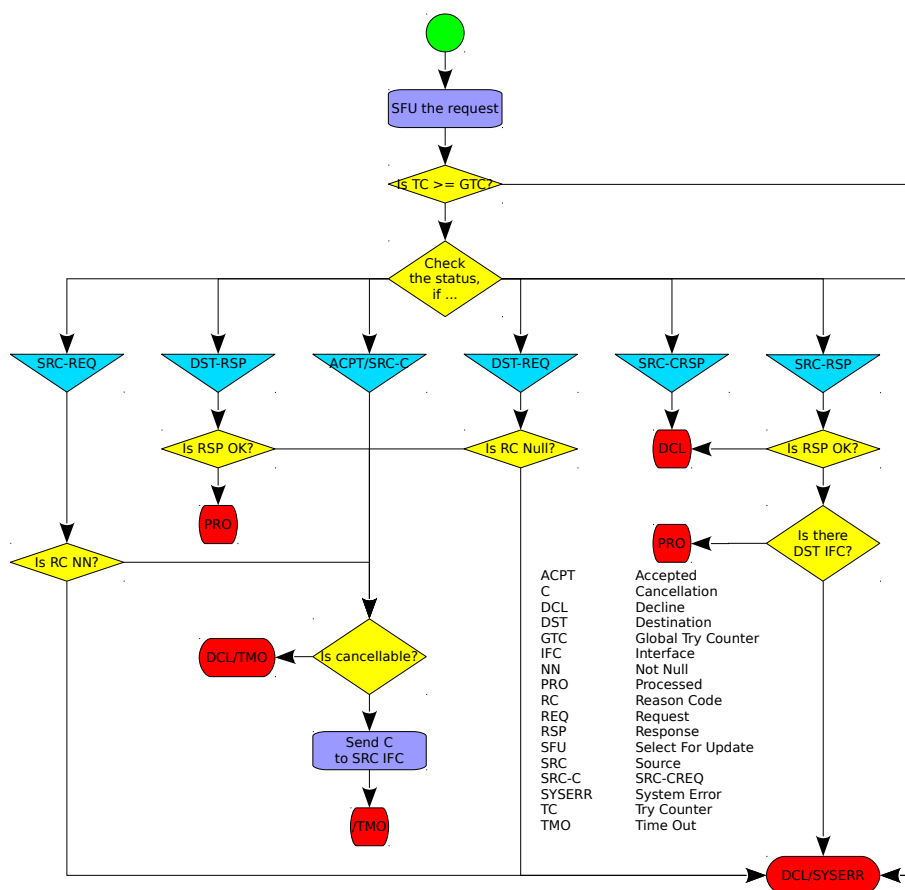
7.2 Исполнение запроса



7.3 Проверка подписи и контракта

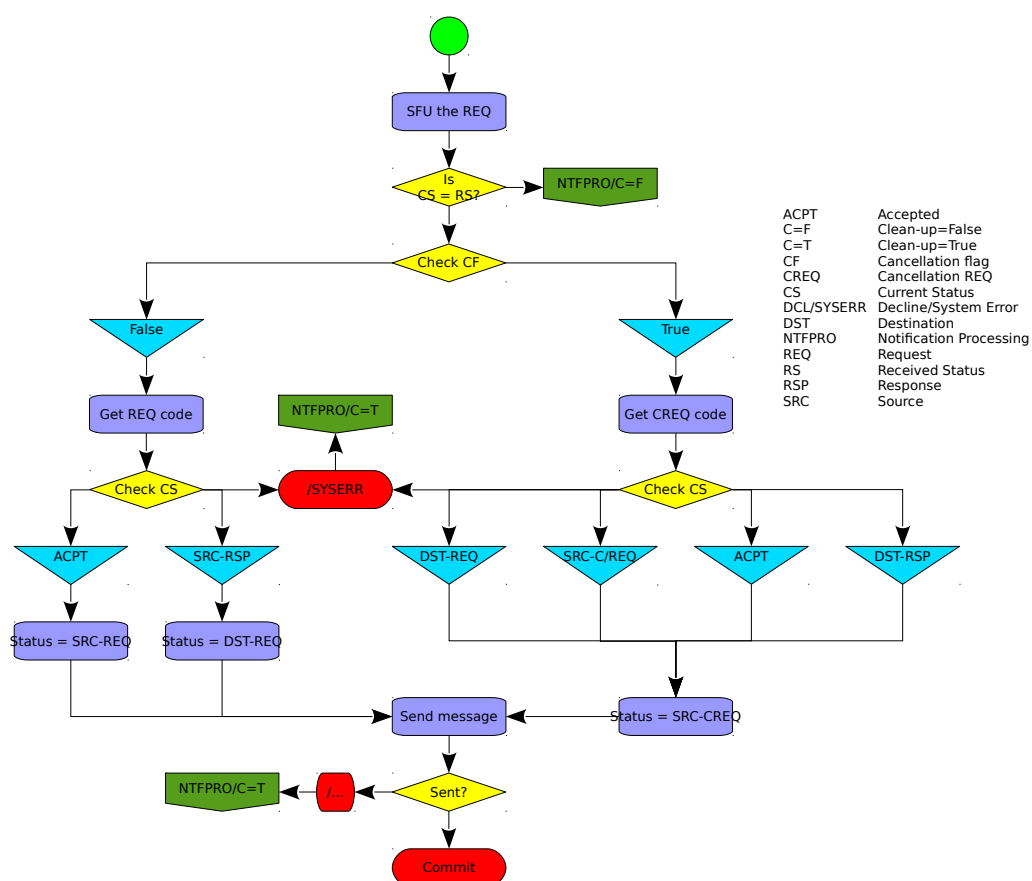


7.4 Отмена запроса



8 Интерфейсы

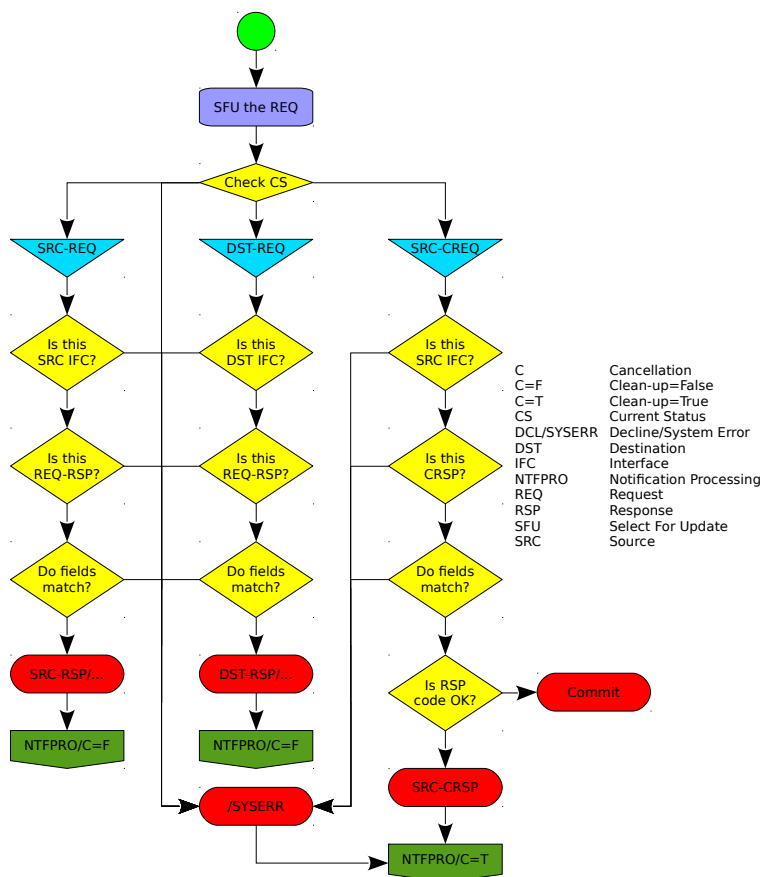
8.1 Запрос



Примечания:

1. при отправке отменяющего запроса интерфейс должен увеличить количество попыток отправок и задержку (в геометрической прогрессии) следующего отправления;
2. проверка успешности отправки не осуществляется для отменяющего запроса.

8.2 Ответ



9 Настройки мидлета

1. «Предопределенные платежи»:
 1. выводиться список платежей;
 2. выводиться три кнопки: «Добавить», «Изменить» и «Удалить»;
 3. в форме добавления и изменения выводятся поля:
 1. наименование*;
 2. № счета отправителя (выводимых по фильтру “S”);
 3. № счета получателя (выводимых по фильтру “R”);
 4. сумма;

5. валюта;
 6. КНП;
 7. описание.
2. «Обновить счета».
 3. «Установить время автоматического завершения мидлета».
 4. «Изменить пароль».

10 Отчетность

- 1.

11 Безопасность

1. Поля, которые не должны логироваться СУБД:
 1. подпись;
 2. СЧ.
2. Алгоритм подписи должен быть необратимым, т. е. на основе хэш функции.
3. Регулярно проводить сканирование на уязвимость по PCI DSS.
4. Доступ к WebLogic серверам только по ХТТПС.
5. На серверах данной системы другие ПО не должны работать.
6. Для ограничения рисков обеспечить возможность определения:
 1. доступных получателей и видов операций;
 2. максимальной суммы и количества операций за период.
7. При приближении СП к пределу создать запись в системном журнале.
8. Если корневые сертификаты распространены в Java ME телефонов, то рассмотреть возможность подписи мидлета.
9. Руководство для пользователя, в части:
 1. незамедлительного извещения банка о факте кражи, утери;
 2. при дальнейшем неиспользовании телефона закрыть договор;
 3. не раскрытия, не хранения пароля;
 4. не использования пароля или фразы коррелирующегося с личными данными;
 5. не использования словарных слов, имен;
 6. при вводе пароля удостовериться, что никто не подсмотрит ни то, что нажато, ни то, что на экране;
 7. социального инжиниринга (никому, даже если представились сотрудниками банка,

- КНБ, не раскрывать пароль, не изменять его по их же требованию и т. д.);
8. не использования одинаковых паролей с другими системами;
 9. выбора настолько сложного пароля, насколько он сможет запомнить;
 10. безопасной загрузки мидлета;
 11. блокирования телефона при неиспользовании, включая автоматического по истечении некоторого времени не активности;
 12. постоянного контроля над телефоном владельцем — ни кому не предоставлять телефон даже на кратковременное пользование;
 13. не загрузки на телефон непроверенного ПО или из неизвестных источников (Java игры и т. д.);
 14. не открывания вложений в email или MMS сообщениях;
 15. проверки беззвучного ввода пароля;
 16. не разглашения факта использования телефона для осуществления финансовых операций;
 17. регулярного обновления ОС (Firmware) телефона;
 18. возможной установки антивирусной программы;
 19. отключения GPRS, EDGE, WiFi, BT, IR, USB, Serial, SD, mini/micro SD и прочих портов и интерфейсов при неиспользовании;
 20. в браузере оставить только TLS;
 21. и т. д.
10. Каждую или только финансовые операции подтверждать СМС уведомлением.
 11. При не совпадении криптограмм создать запись в системном журнале.
 12. При удалении мидлета отчистить персональные данные.
 13. После выполнения криптографических функций, производить очистку переменных, содержащих криптовеличины.
 14. Мидлет должен аутентифицировать ответ хоста.
 15. На WebLogic ограничить Свиту Шифрования для ХТТПС.
 16. На сервере ограничить Свиту Шифрования для ШС.
 17. В мидлете производить проверку Свиты Шифрования ШС и адрес сервера.
 18. Шифровать все межсерверные соединения.
 19. В мидлете адрес сервера должен быть в IP формате, т. к. есть вероятность взлома DNS сервера и, что менее вероятно, возможность подмены настоящего сертификата поддельным (из-за слабости SHA-1) при проблеме человек-посередине.
 20. Минимальная длина для ХТТПС и ШС 2048 бит.

21. Для предотвращения фишинга имя сервера должно быть простым, коротким.
22. Удалить с ХТТПС заголовка ненужную информацию.
23. Возможно, нужно будет фильтровать то, что вводит пользователь в поля Веб формы, дабы исключить SQL инъекцию.
24. Заносить в СЖ все подозрительные ситуации по безопасности.
25. Настройка файерволов должна быть такова, чтобы с серверов системы и приложений можно было обращаться только к БД, АБИСам и между AC1 и AC2.
26. Покупатель может установить IPS и/или IDS.
27. На файерволе включить защиту от DoS атак.
28. Для ХТТПС использовать только TLS с FIPS-approved алгоритмами. В браузере выключить, а в мидлете проверять, что не используется SSL 3.0.
29. Криптомодуль должен быть одобрен против FIPS 140-2.
30. Своевременно обновлять CRLs.
31. Свиты для сервера (вероятно, желательно):
 1. TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA;
 2. TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA;
 3. TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA;
 4. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA;
 5. TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA;
 6. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA.
32. Сервер должен учитывать приоритет свит клиента.
33. Клиент должен проверять сертификационный путь.
34. Клиент должен проверять совпадение имени в сертификате с реальным адресом.
35. Для Cookies должен быть установлен флаг Secure.
36. Выключить TLS renegotiation (no_renegotiation).

12 Обязательства покупателя

1. Не вносит изменения в схему, структуру и системные данные системы.
2. Своевременно устанавливает обновления или заплатки устраняющие уязвимости, предварительно протестировав их.
3. Не устанавливать (удалить) ненужные сервисы, приложения и протоколы.
4. Разработка плана восстановления системы.
5. Периодическое тестирование безопасности.

6. Периодически смотреть логи и извещать поставщика о проблемах.
7. Ограничить количество пользователей серверов (до 2-х).
8. Не использовать сервера для других целей.
9. Удаленное управление серверами должно быть шифрованное.
10. ОС только на базе Юникс.
11. Устанавливать дополнительные меры безопасности, предварительно согласовав с поставщиком.
12. Удалить все ненужные учетные записи всего ПО устанавливаемого на серверах.
13. Изменить значения установленные по умолчанию, которые могут привести к нарушению безопасности системы.
14. Раздавать только необходимые права сотрудникам.
15. Настраивать систему безопасности ПО и оборудования сторонних производителей в соответствии с их документацией.
16. Использовать NTP.
17. Сервер приложений смотрящий наружу должен иметь лишь регистрирующее приложение.

13 Требования системы

1.

14 Чек лист

1. Доступ к серверам должен быть ограничен.
2. Все соединения между серверами должны быть криптографически защищены.
3. Проверена аварийная перезагрузка ключей в криптографический модуль.
4. Наличие всех необходимых валют, т. к. добавление новой валюты потребует переинициализации мидлета.
5. Уведомить покупателя об ограничении в 65 535 попыток операций.
6. Просканировать открытые порты.
7. Сервера защищены файерволами.
8. Мидлет должен загружаться по IP адресу.
9. Персонал для серверов есть, а пользователи обучены работе с системой.
10. Проверить отсутствие SSL 1.0, 2.0, 3.0. Должен быть только TLS с AES/3DES и SHA (желательно 256).
11. На файерволах должны быть открыты лишь порты для настоящей системы и 443.